THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **MOTION TO RECONSIDER ORDER DENYING DEFENDANT'S MOTION TO DISMISS COUNTS 2 THROUGH 8** Noted for May 5, 2022

I. INTRODUCTION

Defendant Paige Thompson, through counsel, moves the Court to reconsider its March 21, 2022 order denying Ms. Thompson's motion to dismiss Counts 2 through 8 for failure to state a claim pursuant to Federal Rule of Criminal Procedure 12(b) and for violations of her Fifth Amendment right to due process and First Amendment right to free speech and expression. (*See* Dkt. No. 226.)

Counts 2 through 8 of the second superseding indictment charge Ms. Thompson with violations of the Computer Fraud and Abuse Act ("CFAA") against various alleged "victim" entities. (Dkt. No. 166.) On December 2, 2021, Ms. Thompson moved to dismiss those counts. (Dkt. No. 123.) The Court heard oral argument on Ms. Thompson's motion on March 15, 2022, and subsequently issued an order denying the motion on March 21, 2022. (Dkt. Nos. 212, 226.) The Court, however, issued this order before the Ninth Circuit issued its ruling in *hiQ Labs, Inc. v. LinkedIn Corp.*, ___ F.4th ___, No. 17-16783, 2022 WL 1132814 (9th Cir. Apr. 18, 2022), on April 18, 2022. The *hiQ* decision directly addressed the standard for "without authorization" under the CFAA, which was previously an unresolved issue by the Ninth Circuit. For the reasons articulated below, that decision strongly supports the dismissal of Counts 2 through 8. In light of *hiQ*, the Court should reconsider its prior ruling and dismiss Counts 2 through 8 with prejudice.

II. RELEVANT FACTS AND PROCEDURAL HISTORY

On January 12, 2022, the grand jury returned a second superseding indictment ("Indictment"), which included ten counts. (Dkt. No. 166.) Counts 2 through 8 charge Ms. Thompson with intentionally accessing a computer without authorization in violation of the CFAA, 18 U.S.C. §§ 1030(a)(2)(A) and (a)(5)(A). (*Id.* at 6-8.)

Count 1 (wire fraud) sets forth the government's vague theory with respect to Counts 2 through 8. (*Id.* at 1-6.) That count alleges that Ms. Thompson utilized "scanners" in an impermissible way. (*Id.* at 3.) As stated in government's filings, the proxy scanners permitted Ms. Thompson to "scan the public-facing portions" of cloud servers owned and operated by Amazon Web Services ("AWS") but rented by Capital One and the other entities. (*See, e.g., id.*) The Indictment alleges that these proxy scanners allowed Ms. Thompson to "identify servers for which the web application firewall misconfigurations permitted commands sent from outside the servers." (*Id.*) According to the Indictment, once Ms. Thompson identified such misconfigurations, she "transmitted commands to the misconfigured servers that obtained the security credentials" belonging to Capital One and the other entities. (*Id.*) After Ms. Thompson obtained these security credentials, the Indictment alleges that she used them to obtain "lists or directories of folders or, buckets, of data," which she then copied to her own server; this data allegedly included "personal identifying information, from approximately 100,000,000 customers who had applied for credit cards from Capital One." (*Id.* at 4.)

The Indictment does not specify the data allegedly obtained from the other entities. (*Id.* at 5.) However, the government's Bill of Particulars describes the data as follows: Victim 2 ("publicly available information"); Victim 3 ("configuration and source code from programming projects"); Victim 4 ("communications data that had been publicly released"); Victim 5 ("log files and customer information including customer names, phone numbers, email address, and applications used . . . encrypted usernames and passwords"); Victim 6 ("metadata, including access logs, firewall logs, and error logs that contained customer phone numbers, emails addresses, IP addresses, and domain names"); Victim 7 ("2.5 million names, phone numbers, addresses, and email addresses, as well as logging data and Linux installers."); and Victim 8 ("metadata describing . . . AWS instances.") (Dkt. No. 232-1 at 2-4.)

In addition to the allegations regarding obtaining data, the Indictment further alleges that Ms. Thompson utilized the security credentials she obtained to then impermissibly use the computing power of the AWS servers rented by Capital One and the other entities to mine cryptocurrency. (Dkt. No. 166 at 5.) The Indictment also alleges Ms. Thompson attempted to use personally identifying information ("PII") taken from AWS's servers to create unauthorized credit and debit cards, and she intentionally and unlawfully possessed the PII of "millions of people." (*Id*. at 4, 8.) As to Counts 2 through 5, the Indictment claims that the value of the information obtained by Ms. Thompson exceeded $5,000. (*Id.* at 6-7.) For Counts 6 and 7, the value of the information is not alleged. (*Id*. at 7.) For Count 8, the Indictment alleges that Ms. Thompson's alleged cryptocurrency mining cost certain entities a loss of over $5,000. (*Id.* at 7-8.)

On December 2, 2021, Ms. Thompson moved to dismiss Counts 2 through 8 pursuant to Rule 12(b) for failure to state a claim, as well as on Fifth Amendment due process and First Amendment free speech grounds. (Dkt. No. 123.) The government subsequently filed an opposition, and Ms. Thompson filed a reply in support of her motion. (Dkt. Nos. 135, 160.) On March 15, 2022, the Court heard oral argument on the motion to dismiss, and on March 21, 2022, issued an order denying it. (Dkt. Nos. 212, 226.) On April 18, 2022, the Ninth Circuit issued its *hiQ* ruling.

III. ARGUMENT

A. The Ninth Circuit's *hiQ* Decision Merits Reconsideration of the Motion to Dismiss Counts 2 Through 8.

Although motions for reconsideration are generally "disfavored," they are appropriate where new "legal authority which could not have been brought to" the Court's attention "earlier with reasonable diligence" is issued. W.D. Wash. Local Crim. R. 12(b)(13). Here, the Ninth Circuit's *hiQ* case, which directly addresses issues pertinent to the motion to dismiss Counts 2 through 8, was not decided until approximately a month *after* the Court's ruling on that motion. Reconsideration is therefore appropriate.

The Court's order found that Ms. Thompson's "most compelling argument" was that she could not have violated CFAA as a matter of law because the information she accessed on the alleged victims' servers was essentially "public." (Dkt. No. 226 at 7-8.) But the Court declined to rule in Ms. Thompson's favor, at least in part, because the Ninth Circuit's earlier decision in *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1003 (9th Cir. 2019), which held that it was "likely that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA," had been "vacated and remanded by the Supreme Court for further consideration in light of *Van Buren*" *v. United States*, 141 S. Ct. 1648 (2021). (Dkt. No. 226 at 7-8.) As the Court noted in its order, lack of authorization is a key element as to *all* of the CFAA violations with which Ms. Thompson is charged. (*Id.* at 3.)

The Ninth Circuit has now made clear, after its consideration of *Van Buren*, that there can be no viable CFAA charge in the absence of a "password-protected" server or a server "that otherwise prevent[s] the general public from viewing [its] information." *hiQ*, 2022 WL 1132814, at *13. As a result, the Court should reconsider its ruling and dismiss the CFAA charges.

B. The Ninth Circuit's *hiQ* Decision Requires Dismissal of Counts 2 Through 8 Because the Alleged Victims' Servers Had No Authentication Requirement.

The facts and reasoning of *hiQ* are squarely applicable to the pending CFAA charges against Ms. Thompson and weigh strongly in favor of dismissal. In *hiQ*, a social media company named LinkedIn attempted to stop its competitor, hiQ, from "scraping"[1] information from LinkedIn's user profiles. *Id.* at * 3. Although LinkedIn pages are generally accessible to the public, LinkedIn took various anti-scraping measures including prohibiting unauthorized bots, such as those employed by hiQ, to access its servers and deploying "several technological systems to detect suspicious activity and restrict automated scraping." *Id.* Although LinkedIn blocks "approximately 95 million automated attempts to scrape data every day, and has restricted over 11 million accounts suspected of violating its User Agreement, including through scraping," its countermeasures against hiQ were insufficient and so, in May 2017, it sent hiQ a cease-and-desist letter threatening to sue hiQ for, among other things, violations of the CFAA. *Id.* at *3-4. Thus, hiQ clearly did not have *permission* to scrape data from LinkedIn's servers, just as the government has consistently claimed that Ms. Thompson did not have the alleged victims' *permission* to similarly access their data.

[1] Scraping is the process of "extracting data from a website and copying it into a structure format," usually by an automated web robot or "bot." *hiQ*, 2022 WL 1132814, at *3 n.4.

Relying on the reasoning in *Van Buren,* however*,* the Ninth Circuit clarified that a lack of *permission* and a lack of *authorization* are quite different in terms of the CFAA's applicability. Indeed, the Ninth Circuit found in *hiQ* that where computer access "is open to the general public, the CFAA 'without authorization' concept is inapplicable." *Id.* at *12. That is precisely the case here (*i.e.,* anyone could have accessed the alleged victims' data at issue), which the government cannot and does not dispute.

The Ninth Circuit further explained that when applying *Van Buren*'s "gates" analogy, publicly available servers have "erected no gates to lift or lower in the first place." *Id.* at *14. That is true even where the server's owner wants to selectively restrict access to the otherwise public server because where the "default is free access without authorization in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of authorization." *Id.* at *12. As a result, the Ninth Circuit held that "authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information." *Id.* at *13. In other words, only a technological act analogous to "breaking and entering" can justify a CFAA charge. *Id.* at *12, 13 (discussing the CFAA's legislative history).

Cases in which an individual circumvents a secure computer system (*i.e.*, where "authorization generally is required and has either never been given or has been revoked") may have a viable CFAA claim. *See, e.g., id.* at *15 (discussing *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016), which involved password fraud, and *Facebook, Inc. v. Power Ventures*, *Inc.*, 844 F. Supp. 2d 1025 (N.D. Cal. 2012), which involved circumventing a password-protected authentication system). Conversely, in cases where server information is "presumptively open to all comers," even where the server's owner attempts to selectively limit access, no CFAA violation occurs. *hiQ*, 2022 WL 1132814, at *15 (*quoting Power Ventures*, 844 F.3d at 1067 n.2). This interpretation of the CFAA is consistent with the Ninth Circuit's interpretation of the Stored Communications Act ("SCA"), 18 U.S.C § 2701 *et seq.*, which protects solely "electronic communications that are configured to be private and are not intended to be available to the public." 2022 WL 1132814, at *16.

There is no substantive difference between the webpages in *hiQ* and the alleged victims' servers in this case. LinkedIn's webpages were publicly accessible to anyone with a web browser, and the alleged victims' servers here were publicly accessible to anyone with a proxy scanner (itself also publicly available). *See id.* at *6. LinkedIn tried various methods to limit access to its servers by scrapers that, ultimately, were as ineffective as the methods (if any) the alleged victims took here. *See id.* at *3. Specifically, LinkedIn utilized: (a) FUSE system to scan and impose limits of user activity; (b) Quicksand system to monitor patterns of access to LinkedIn's servers; (c) Sentinel system to scan and block suspicious activity associated with specific Internet Protocol ("IP") addresses; (d) Org Block system, which identifies scrapers and blocks their IP addresses; (e) request scoring systems, which monitor and restrict activity indicative of bots; and (f) a "robots.txt" file, which attempts to prohibit automated programs used by scrapers. *HiQ Labs, Inc. v. LinkedIn Corp.*, 2017 WL 4518160, at *7 (9th Cir. April 18, 2022) (Op. Br. of LinkedIn Corp.). Frankly, hiQ bypassed far *greater* security measures than the Indictment alleges Ms. Thompson did (not that any were really bypassed, as explained below), and yet the Ninth Circuit held the CFAA did not apply to hiQ's conduct.

HiQ and Ms. Thompson both wrote and executed code that allowed them to access the publicly available information *because and only because* neither LinkedIn nor the alleged victim entities ever employed an individualized authentication system that determined which persons were authorized to access and download data (*e.g.,* password, two-factor authentication, PIN, biometric authentication, , etc.).[2] In other words, neither LinkedIn nor the alleged victim entities in this case ever put a gate on their computer servers, much less opened a gate. As such, Ms. Thompson cannot be found liable—as a matter of law—for a CFAA violation and Counts 2 through 8 must be dismissed.

During oral argument, the government tried to utilize several exhibits to establish that Ms. Thompson "stole" security credentials from the alleged victim servers. (*See* Dkt. No. 212 ("Gov't Ex.") at Exs. 1-6.) But this presentation was misleading and sowed unnecessary confusion. When those exhibits are examined carefully, they actually support the conclusion that the CFAA charges against Ms. Thompson must be dismissed, even when viewing the Indictment's allegations in the light most favorable to the government.

The "security credential" that Ms. Thompson is alleged to have exploited is an "iam/role." (*See* Gov't Ex. 6). "AWS Identity and Access Management (IAM) lets [users] manage several types of long-term security credentials for IAM users." (*Manage IAM credentials*, AWS, *available at* https://aws.amazon.com/iam/features/managing-user-credentials/ (last checked May 4, 2022).) IAM is not actually a true security credential, particularly when viewed through the lens of the *hiQ* decision. An IAM role is "an AWS identity with permission policies that determine what the identity can and cannot do in AWS." (*IAM roles*, AWS, *available at* https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html (last visited May 2, 2022).) However, an IAM role is not "uniquely associated with one person" and does not have "standard long-term credentials such as a password or access keys." (*Id.*) Instead, "when you assume a role,

[2] Specifically, the Indictment alleges "scanners that allowed her to scan the public-facing portion of servers…, [allowed her] to identify servers for which web application firewall misconfigurations permitted commands sent from outside the servers to reach and be executed by the servers." (Dkt. No. 166 at 3.)

it provides you with the temporary security credentials for your role session." *Id.* In other words, once the system gives a requesting computer the IAM role, the security credentials are given automatically—they are not "stolen."

AWS users can choose to utilize the IAM role to "delegate access to users, applications, or services that don't normally have access to [that users'] AWS resources." (*Id.*) In other words, Capital One and the other alleged victims (a) created IAM roles; (b) defined which accounts or AWS servers could assume the IAM role; (c) defined which actions and resources the IAM role could access; and (d) allowed for the provision of temporary security credentials to be *automatically* assigned to the IAM role. (*IAM roles for Amazon EC2*, AWS, *available at* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (last visited May 2, 2022).)

Ms. Thompson played no part in determining how the alleged victim entities created and defined their IAM roles, nor did she forcibly "break and enter" the IAM role—it was automatically given to the requesting computer by utilizing a simple, publicly known and publicly published command. (*See* Dkt. No. 212, Gov't Exs. 1, 3 (providing the exact code snippet the government alleges Ms. Thompson used as an example of how to retrieve IAM security credentials).) Indeed, the code that the government showed the Court during the hearing, Gov't Ex. 2, is publicly accessible in AWS's online documentation for how to "use temporary security credentials" with AWS. (*See Using temporary security credentials with the AWS CLI*, AWS, *available at* https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_use-resources.html (last visited May 2, 2022).)

Ms. Thompson also had *no* say in what resources the IAM role would access and what data would be made available to whom. The alleged victim entities could have programmed that IAM role to access *nothing*. Instead, as but one example, Capital One programmed its IAM role in a way that made large swaths of its data available to anyone. At Capital One's elections, some of the data happened to contain PII, but much of it did not.[3] Other alleged victims allowed public access and copying of otherwise publicly available data. Because the alleged victim entities configured (or misconfigured) their servers to act as proxies and allowed *any computer in the world* to obtain an IAM role, once Ms. Thompson's computer allegedly accessed the purported victims' servers, it was automatically authorized to access the victims' data. Put simply, there was no gate.

During argument, the government made much of the verbiage "AWS_SECRET_ACCESS_KEY" to argue that something labeled "SECRET" must invariably be "stolen." (*See* Dkt. No. 221 [March 15, 2022 Tr. at 12, 25].) But that verbiage is simply programming language that AWS uses. A word utilized in computer programming language does not necessarily share the same meaning as the same word in the English language. And that is the case here. While the conversational English language definition of the word "secret" is "kept from knowledge or view,"[4] that is not its definition in computer programming language. Rather, in programming, the variable "SECRET_ACCESS_KEY" is an *indication to programmers* that they should only configure the system to give the key to computers they want to authorize. The fact that the alleged victims' servers were set up to give the "SECRET_ACCESS_KEY" to any individual (or bot or computer system) is a programmatic indication that Ms. Thompson's alleged access was *authorized*, and therefore it cannot, as a matter of law, substantiate a CFAA charge.

[3] *See* Dkt. No. 155-2, *Capital One's Memorandum of Law in Support of Its Motion to Dismiss the Representative Consumer Class Action Complaint* at 16, *In Re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19-md-2915-AJT-JFA, (E.D.Va. April 10, 2020).

[4] https://www.merriam-webster.com/dictionary/secret

In short, Ms. Thompson did not steal anything; once she purportedly accessed the alleged victims' servers through a publicly accessible port, those AWS servers gave her computer the IAM role and generated temporary security credentials without further authentication or challenge. That is far *less* protection than LinkedIn provided its own servers which, while publicly accessible, at least had some technological countermeasures deployed to stop scrapers like hiQ. LinkedIn could not sustain a CFAA claim against hiQ, and the government similarly cannot do so against Ms. Thompson.

C. The Ninth Circuit's *hiQ* Decision Requires Dismissal of Counts 2 Through 8 Because the Rule of Lenity Prohibits Such Charges.

The Court should also reconsider its ruling based on the Ninth Circuit's determination in *hiQ* that the rule of lenity requires the CFAA's "without authorization" provision to be interpreted "narrow[ly] . . . so as not to turn a criminal hacking statute into a 'sweeping Internet-policing mandate." 2022 WL 1132814, at *16. The rule of lenity weighs heavily in favor of dismissing the CFAA charges against Ms. Thompson.[5] (*See generally*, Dkt. No. 123 at 8-13.)

Here, just as hiQ was aware that LinkedIn did not want it to access its publicly available servers, Ms. Thompson may have been aware that she was not necessarily the user who should have been designated an IAM role by the alleged victim servers. Regardless, such knowledge does not change the "without authorization" requirement of the CFAA. To the extent there is an ambiguity in the CFAA regarding such authorization requirement, it must be strictly construed against the government. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009). If there is "any doubt" about whether Congress intended the CFAA to prohibit the conduct in which Ms.

[5] That is especially true here, where the application of the CFAA as to Ms. Thompson also implicates her free speech rights under the First Amendment and her due process rights under the Fifth Amendment (as the defense explained in the underlying motion to dismiss and reply in support of it).

Thompson engaged, then the Court "must choose the interpretation least likely to impose penalties unintended by Congress." *United States v. Nosal*, 676 F.3d 865, 863 (9th Cir. 2012). This is true regardless of what Ms. Thompson, who was suffering from mental health issues at the time, might have thought privately to herself or shared on social media. In the absence of circumvention of a password-protected or otherwise restricted system, charging Ms. Thompson with a violation of the CFAA violates the rule of lenity. Moreover, as the defense previously noted, and *hiQ* makes even clearer, the government's interpretation of the pertinent CFAA provisions captures helpful and common white hat hacker behavior. (*See, e.g.,* Dkt. No. 160 at 5.)

The Court should reconsider its prior ruling and dismiss the CFAA charges on this separate ground.

IV. CONCLUSION

For all of the above-stated reasons, the Court should grant Ms. Thompson's motion for reconsideration and dismiss Counts 2 through 8 of the Indictment with prejudice.

DATED: May 5, 2022

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Christopher Sanders*
CHRISTOPHER SANDERS
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson